TV Web Dream

Navigation Menu

Des milliers de sites WordPress piratés !

Publié le 31, juil, 2014 | 0 commentaires

Tout a commencé par un appel téléphonique samedi 12 juillet, un de mes clients me prévient que son site est indisponible. Son site n'est pas hébergé sur mes serveurs privés et je n'en fais pas la maintenance. Après une première vérification, il s'avère qu'un processus se sert de son hébergement comme d'un point de départ pour le spamming (envois massifs de mails).

Malgré une tentative de nettoyage, il a bien fallu me rendre à l'évidence, il allait falloir que je recharge intégralement le core de WordPress ainsi que tous ses plugin et que je vérifie que rien ne traîne dans le répertoire uploads.

Seulement en parcourant le web, j'allais apprendre que mon client est loin, très loin d'être le seul dans ce cas. En effet un piratage massif des sites sous WordPress venait de se dérouler. À première vue, peu importe le

type d'hébergement (mutualisé ou privé), les thèmes ou les plugin utilisés. Même si l'éditeur Sucuri a rapidement pointé du doigt le plugin de newsletter MailPoet. Il existe en fait plusieurs plugin impactés par des failles qui ont permis cette attaque massive. En voici une liste non exhaustive :

- Gallery Objects 0.4 SQL Injection
- WPTouch Authenticated File Upload
- CopySafe PDF Protection 0.6 Shell Upload
- Tidio Gallery 1.1 Shell Upload / XSS
- Download Manager 2.6.8 Shell Upload
- BSK PDF Manager 1.3.2 SQL Injection
- MailPoet wysija-newsletters Unauthenticated File Upload
- NextGEN Gallery 2.0.63 Shell Upload
- blogstand-smart-banner.1.0 Cross Site Scripting
- ml-slider 2.5 Cross Site Scripting
- wp-construction-mode.1.8 Cross Site Scripting
- Simple Share Buttons Adder 4.4 CSRF / XSS

Pas grave diront certains, il suffit d'utiliser une sauvegarde pour restaurer mon site. Et là je dis ERREUR ! Car les fichiers malicieux peuvent être présents depuis plusieurs mois de manière silencieuse sur votre site. De ce fait vos sauvegardes ont donc de

grandes chances d'êtres infectées….

Il ne reste plus aux possesseurs de sites infectés (ou à leur webmaster) qu'à nettoyer leur base de données, et surtout, supprimer tout ce qui est core, thème, plugins, et réuploader le tout au propre avec les dernières versions.

Premier conseil : Bloquez l'accès à votre site !

En effet vous ne voulez pas qu'un hacker ou un visiteur accède à votre site pendant que vous tentez de le nettoyer. Pour cela il suffit simplement de créer un fichier .htaccess avec le code suivant :

order deny,allow
deny from all
allow from !!Votre IP ici!!

Il suffit d'indiquer votre adresse IP à la place de « Votre IP ici » pour autoriser l'accès du site à vous et vous seul !

Deuxième conseil : Protégez votre dossier uploads !

Vérifiez qu'aucun fichier ne traîne dans votre répertoire uploads et insérer ensuite un fichier .htaccess avec le code suivant :

*<Files *.php>*
Deny from all
</Files>

Options – Indexes

Cela aura deux effets, empêcher l'exécution de script PHP et empêcher de

cataloguer le contenu de vos dossiers.

Je souhaite bon courage à ceux ou celles qui sont en train de tenter de récupérer leur site…

Sujets en rapport

Le TV Web Dream nouveau est arrivé !

Modifications sur le site

La page Facebook TV Web Dream

Générique de TV WEB DREAM

Cédric Louis Calibreur ISF

Tutoriel Foobar : SACD (Super Audio CD)

Auteur: Cédric Giannone

Laisser un commentaire

Nom *

E-Mail *

Commentaire

Soumettre

Chercher sur le site

Recherche pour :

Rechercher

Articles récents

- Humble Bundle Square Enix
- Des milliers de sites WordPress piratés !
- Le TV Web Dream nouveau est arrivé !
- Test Intel NUC
- Test : la nouvelle Box Numericable

Commentaires récents

- Cedric dans Tutoriel XBMC : le mode portable
- christophe dans Tutoriel XBMC : le mode portable
- Cedric dans Tutoriel Foobar : contrôle via Android
- jean dans Tutoriel Foobar :

contrôle via Android

- TTBR dans Tutoriel VirtualBox : initiation avec une machine virtuelle Ubuntu 13.10

Réalisé par **CG Info Services** | © 2014 **TV Web Dream**